



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/042,038	01/07/2002	Steven Francis Best	AUS920011030US1	6968

7590 09/02/2005

International Business Machines Corporation
Intellectual Property Law Department,
Internal, Zip 4054
11400 Burnet Road
Austin, TX 78758

EXAMINER

HERRING, VIRGIL A

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 09/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

87

Office Action Summary

Application No.

10/042,038

Applicant(s)

BEST ET AL.

Examiner

Virgil Herring

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 January 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 07 January 2002 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>1/7/2002</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is responsive to the communication filed on January 7, 2002. Claims 1-14, representing a system and method for generating passwords for a user to access a resource, are pending. At this time, claims 1-14 are rejected.

Drawings

2. The drawings are objected to because they are hand drawn and of poor quality. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

3. The disclosure is objected to because of the following informalities:
4. Pages 1, 3, and 20 refer to a copending application by the internal docket number AUS920010598US1. Please replace this with the appropriate USPTO application number. The examiner has determined that the USPTO designation is 10/042,095.
5. Page 13, line 20 reads "The set of global hash keys 420 (Fig. 4) generate the". The verb "generates" should be used instead, since the noun of the sentence is the set, rather than the keys.
6. Page 19, line 6 refers to "Fig. 5", which does not exist. Based on the references to items 515-518, it appears that line 6 should refer to Fig. 5B.
7. In several places in the specification and claims (such as page 21, line 6) applicant has used the phrase "user id". The examiner suggests changing this to "user ID" to indicate that it is short for user identification.
8. Appropriate correction is required.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claims 1-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kumhyr (US2003/0041251) in view of Barret, et al.

11. As per claims 1, 6, 9, 11, 12, and 14, Kumhyr (US2003/0041251) discloses a method for generating a password for a user for access to a resource having a unique resource name, comprising:

- i) receiving as input, from a user, a user global password, a user id, and at least one hash key; (Column 3 Lines 35-38, 40-42)
- ii) determining the resource name of the resource; (Column 3, Lines 40-42)
- iii) generating the password based upon the global user password, the resource name and the hash key during a first communication session with the resource; and (Column 3, Lines 40-42)

Art Unit: 2132

iv) regenerating the password during a next communication session with the resource by repeating steps i, ii, and iii. (Column 3, Lines 46-48)

AND a method for generating a password for a user for access to an Internet site having a domain name, comprising:

receiving as input a user global password, a user id, and a set of hash keys;

(Column 3, Lines 35-42, 48-52)

determining a domain name of the Internet site; (Column 3, Lines 40-42)

determining an iteration of password renewal for the Internet site; (*)

determining a corresponding hash key to the determined iteration; and (*)

generating the password based upon the global user password, the domain name, and the corresponding hash key wherein the generated password is regenerated during a next communication session with the Internet site by the user. (* Column 3, Lines 48-52; See explanation below)

12. On page 2, paragraphs [0020] and [0024], Kumhyr (US2003/0041251) discloses the process by which passwords are generated in his system. The user supplies a preferred word (clearly an easily remembered password) to the system. Though not expressly disclosed, official notice is taken that a password is typically paired with a user ID. Therefore, it would be obvious to one skilled in the art to include the user ID with the preferred word for the purpose of password generation. The motivation for doing so would have been for the target application to have a name to associate with the password being provided.

13. Kumhyr (US2003/0041251) also discloses, in paragraph [0007] of page 1 that, "the invention may be implemented in a way that emphasizes security." He lists several symmetric encryption algorithms that can be applied to the password for security, such as Blowfish, DES, IDEA, RC2, and RC4. Barret, et al disclose the use of these same encryption algorithms in ssh connections. They also list several other algorithms used by ssh, such as RSA, DSA, DH, CRC-32, MD5, and SHA-1. It would have been obvious to one skilled in the art that if a symmetric encryption algorithm can be used in password encryption (Kumhyr), then using other algorithms of similar security are equally valid methods of encrypting a password. The motivation for doing so would have been to increase security for the user by disguising an easily-remembered preferred word as something which appears to be nothing more than random characters to prevent the password from being easily guessed.

14. With regards to the "set of hash keys" in claims 6-8, 11, and 14, Kumhyr (US2003/0041251) discloses in paragraph [0020] that "an optional feature may allow user 210 to continue the same input at 220, but to direct a change in the algorithm used by password generator 230, and thus change the output at 260, when a password needs to be changed." In a hashing algorithm, the hash key is treated as a constant value relative to the other inputs. In this case, a hash key relating to a specific user ID, password, and application would be a constant in the equation the hashing algorithm evaluates. Those skilled in the art will note that the easiest way to alter a hashing algorithm while maintaining the same level of security would be to change the hash key

Art Unit: 2132

being used. The motivation for doing so would be to generate a different encrypted password from the same user ID and preferred word. Thus, it would have been obvious to those skilled in the art to use more than one hash key (i.e., a set) as input to the password generator, for the purpose of generating a new password when the current one expires.

15. As per claims 2 and 3, Kumhyr (US2003/0041251) discloses the method of claim 1 wherein the resource is an Internet site having a unique domain name; or wherein the resource is an application and the resource name is an application name. (Column 3, Lines 40-42)

16. Paragraph [0020] of page 2 states that once generated, the invention "provides, 260, the password to a target application 270." On page 1, paragraph [0017], Kumhyr describes an application to be "any program or function including voice mail, e-mail, online banking, accounting software, or a web site function." Thus, Kumhyr anticipated that the resource to which the password is provided could be "an Internet site having a unique domain name" (claim 2) or "an application" (claim 3). It is known to those skilled in the art that all Internet sites have unique domain names. Furthermore, it is inherent that providing a password to any application would necessarily involve identifying the name of the application to be used.

Art Unit: 2132

17. As per claims 4, 7, 10, and 13, Kumhyr (US2003/0041251) discloses the method of claim {1, 9, or 12} further comprising automatically populating the resource with the generated password and user ID. (Column 3, Lines 40-42)

18. In paragraph [0020] on page 2, Kumhyr (US2003/0041251) states, "Password generator 230 translates the preferred word to produce a password, and provides, 260, the password to a target application 270." Thus, the password is automatically transferred to the application being used. In other words, the password field for the application is automatically populated by the generated password. As noted above (in paragraph 12), passwords are paired with user IDs, so it would be obvious to one skilled in the art to automatically populate the application with the user ID as well. The motivation for doing so would have been for the application to have a name to associate with the password, and thus authenticate the user.

19. As per claims 5 and 8, Kumhyr (US2003/0041251) discloses the method of claim 1 further comprising determining if the resource has a format requirement for a password; and conforming the generated password to the format requirement in a consistent manner whereby the conformed generated password is regenerated during a next communication session with the resource by the user. (Column 3, Lines 38-40)

20. In paragraph [0020], Kumhyr (US2003/0041251) states, "Password generator 230 also receives, 250, password format rules based on rule set 240." It is inherent that

to the invention that receiving a set of password format rules will result in the generation of a password that conforms to those rules. Furthermore, in the same paragraph, it is disclosed "the same input at 220 will result in the same output at 260 time after time." Thus, for a given user ID, preferred word (master password), rules set, and application, the invention will always generated the same password.

Conclusion

21. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The prior art listed refers in one way or another to password management.


22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Virgil Herring whose telephone number is (571) 272-8189. The examiner can normally be reached on Monday-Friday.

23. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2132

24. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

VH


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100